UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/527,570	03/10/2005	Markus Bockes	WACHP006	7328

25920 7590 02/18/2010

MARTINE PENILLA & GENCARELLA, LLP
710 LAKEWAY DRIVE
SUITE 200
SUNNYVALE, CA 94085

EXAMINER	
SHIFERAW, ELENI A	

ART UNIT	PAPER NUMBER
2436	

MAIL DATE	DELIVERY MODE
02/18/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/527,570	BOCKES ET AL.	
	Examiner	Art Unit	
	ELENI A. SHIFERAW	2436	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 November 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,14-20,22-32 and 34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,14-20,22-32 and 34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1, 14-20, 22-32 and 34 are pending.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on 12/29/2008 has been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and previously attached.

Response to Amendment

3. The objection to claims 30-31 is withdrawn.

4. The objection to claims 32 and 34 is withdrawn.

5. The 101 rejection to claims 27-29 is withdrawn.

6. The 101 rejection to claims 30-31 is withdrawn.

Response to Argument

7. Applicant's arguments are fully considered but are not persuasive.

8. The applicant's teaching to the examiner regarding what has not done and what needs to be done is noted and appreciated however every single limitation is reasonably addressed in the previous office action by the various paragraphs. The examiner is not trying to teach the invention but is merely trying to interpret the claim language in its broadest and reasonable meaning.

Regarding argument the references failure to teach "(1) a key with at least two key parameters is drawn on, wherein (1.1) the key is a private key for use in an RSA method, wherein (1.2) each key parameter is contained in the private key, wherein (2) an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, wherein (3) the cryptographic calculation is one of a decryption in the RSA method and a signature generation in the RSA method, and wherein (4) each operation of the method for protected execution of the cryptographic calculation is executed by an integrated circuit" argument is not persuasive because Walmsley discloses a checksum register used to verify that k1 and k2 have not been altered by an attacker. The checksum is programmed along with k1, k2, and R with the authentication chip's SSI command. (see par. 944). Walmsley also teaches using asymmetrical encryption algorithm allows the **ChipT** portion of system to be insecure and therefore protocol p2 uses asymmetric cryptography. Each **Chip** contains values of ktChipT (see par. 486-489). See further (par. 652, and 57-66). Therefore, Walmsley clearly discloses in some cases protocol P2

uses asymmetric cryptography to secure and **each chip** containing Kt ChipT only. Public key for encrypting and does not have to be secret; and the key is private key for use in asymmetric algorithm. See also par. 0944 for parameters (k1 and k2) contained in private key.

9. Regarding argument Walmsley teaches RSA method on par. 75-78 but not cited by the examiner, argument is not persuasive because the examiner argues that the examiner not only cited but also explained in many places of the previous office action "asymmetric algorithm". Asymmetric algorithm is RSA method.

10. Regarding argument Walmsley disclosing DSA and ElGamal methods, argument is not persuasive because having extra teaches in Walmsley does not mean the limitations are not taught as recited.

Therefore applicant's arguments regarding references failure to teach:
"(1) a key with at least two key parameters is drawn on, wherein
(1.1) the key is a private key for use in an RSA method, wherein
(1.2) each key parameter is contained in the private key, wherein
(2) an integrity check of the key is performed in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter, wherein

(3) the cryptographic calculation is one of a decryption in the RSA method
and a signature generation in the RSA method, and wherein

(4) each operation of the method for protected execution of the cryptographic
calculation is executed by an integrated circuit," are not persuasive as explained above or Walmsley discloses asymmetric encryption algorithm/RSA, P2 using asymmetric cryptography and chips, EACH CHIP contains the Kt ChipT values, generating checksum integrity check to verify the K1 and K2 of the Chip in order to prevent a cryptographic attack. **(see par. 0486-0489; 0057-0066; *0944*, 0628, 0629, and 0652; 0657, 0954-0957, 0545, 0601-0606).**

11. Therefore, sufficient motivation to combine is provided and the examiner asserts that the system of the prior art teach or suggest the subject matter as recited in independent claims. Dependent claims are also rejected at least by virtue of their dependency on independent claims

and by other reason set forth in this office action dated 08/21/2009. Accordingly, rejections for all pending claims are respectfully maintained.

Claim Rejections - 35 USC § 103

12. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

13. Claims 1, 14-15, 17, 19-22, 25, 27, 30, and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable Walmsley US PG Pubs 20030159036 in view Sabin USPN 6959091 B1.

As to claim 1, Walmsley discloses a method for protected execution of a cryptographic calculation, in which a key with at least two key parameters is drawn on, wherein the key is a private key for use in an RSA method, **wherein each key parameter is contained in the private key (see par. 0486-0489; Use of an asymmetrical encryption algorithm allows the ChipT portion of System to be insecure. Protocol P2 therefore, uses asymmetric cryptography …For this protocol, each chip contains the following values: … Kt ChipT only. Public key for encrypting … see also 0057-0066)**, wherein an integrity check of the key is performed **(see *0944*, 0628, 0629, and 0652; K1, … K2, R, … M)**, in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter wherein each operation of the method for protected

execution of the cryptographic calculation is executed by an integrated circuit **(0657, 0954-0957, 0545, 0601-0606)**.

Walmsley discloses calculating random numbers and generating signature for the random number and calculating signature for decrypted random number **(see 0335-0350)** but does not explicitly teach and wherein the cryptographic calculation is one of a decryption in an RSA method and a signature generation in an RSA method.

However, Sabin discloses wherein the cryptographic calculation **(col. 8 lines 3-67; generating parameters p, q, kp, kq for private key)** is one of a *decryption* in an RSA method and a signature generation in an RSA method **(col. 4 lines 4-67 and col. 7 lines 59-67)**.

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to modify the teachings of Sabin within the system of Walmsley because they are analogous in cryptography calculation. One would have been motivated to combine the teachings to further secure the RSA calculation.

As to claim 14, Walmsley discloses the method as claimed in claim 1, wherein in the integrity check it is determined whether the value of at least one key parameter is contained in a range of valid values, wherein the range is non-contiguous in that it has a plurality of gaps (Walmsley page 40, paragraph 0998).

As to claim 15, Walmsley discloses the method as claimed in claim 1, wherein in the integrity check it is determined whether at least two key parameters are in a predetermined relationship to one another (Walmsley page 40, paragraph 0998).

As to claim 19, Walmsley discloses the method as claimed in claim 1, wherein in the integrity check a checksum stored with the key parameters is compared with a checksum newly

calculated after passing of the key parameters (Walmsley page 13, paragraphs 0036-034 and page 14, paragraph 0036).

As to claim 20, Walmsley discloses the method as claimed in claim 1, wherein, to check the integrity, important parameters to be passed are multiply passed and checked for identity after passing (Walmsley page 13, paragraphs 0036-034 and page 14, paragraph 0036).

As to claim 22, the modified Walmsley discloses the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein the RSA method is an RSA-CRT method.

However, Sabin discloses wherein the RSA method is an RSA-CRT method (col. 8 lines 42-52).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings because the RSA-CRT is a well know cryptographic calculation and to use these protected calculations would increase there security.

As to claim 25, Walmsley the method as claimed in claim 1 wherein the prime factors of the RSA method are multiplied by a masking parameter and the error freedom of the calculation sequence is checked by an equality check modulo the masking parameter (Walmsley page 4, paragraph 0089).

As to claims 27, 30 and 32, claims 27, 30 and 32 encompass the same scope of the invention as those of claims 1 and 26 with the additions of "computer readable storage medium" (Walmsley page 53, paragraph 1297) and portable data carrier (Walmsley page 4, paragraph 0098: smart card).

14. **Claims 16-18, 23-24, 26, 28-29, 31 and 34 are rejected under 35 U.S.C. 103(a) as being unpatentable Walmsley US PG Pubs 20030159036 in view Sabin USPN 6959091 B1. and further in view of Ngo US PG Pubs 20030097628.**

As to claim 16, the modified Walmsley discloses the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein the integrity check includes a multiplicative operation, in particular a divisibility test.

However, Ngo discloses wherein the integrity check includes a multiplicative operation, in particular a divisibility test (Ngo page 1, paragraph 0009).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Ngo within the combination system because to use a divisibility test for an integrity check is a cheaper and a faster calculation (Ngo page 1, paragraph 0009).

As to claims 17 and 28, the modified Walmsley discloses the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein in the integrity check it is checked whether at least one of the key parameters is evenly divisible by a safeguard value.

However, Ngo discloses wherein in the integrity check it is checked whether at least one of the key parameters is evenly divisible by a safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings to again the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred (Ngo page 2, paragraph 0026).

As to claim 18, the modified Walmsley discloses the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein in the integrity check it is checked whether at least one value which differs from one of the key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value.

However, Ngo discloses wherein in the integrity check it is checked whether at least one value which differs from one of the key parameters by a multiple of a safeguard value is evenly divisible by the safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 2, paragraph 0026).

As to claim 23, the modified Walmsley discloses the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value.

However, Ngo discloses wherein in the cryptographic calculation at least one exponentiation operation is performed and in the integrity check it is checked whether the exponent used in the exponentiation operation is evenly divisible by a safeguard value (Ngo page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred (Ngo page 2, paragraph 0026).

As to claim 24, the modified Walmsley discloses the method as claimed in claim 23. The modified Walmsley does not explicitly teach wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying.

However, Sabin discloses wherein in the cryptographic calculation an exponent blinding method is applied for protection against spying **(col. 9 lines 10-29)**.

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine the teachings because to add another multiple as a blinding factor increases the security of the protected calculation.

As to claims 26, 29, 31 and 34 the modified Walmsley discloses the method as claimed in claim 1. The modified Walmsley does not explicitly teach wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check.

However, Ngo discloses wherein at least one key parameter is the product of a value required for the cryptographic calculation times a safeguard value, and wherein the integrity check includes a divisibility check (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

It would be obvious to one of ordinary skill in the art at the time of the applicant's invention to combine Walmsley and Ngo because the divisibility check is cheaper and faster as well as if you use a predetermined value it adds to the assurance that there are no errors or whether or not corruption has occurred and to add another multiple as a blinding factor increases the security of the protected calculation (Ngo page 1, paragraph 0009 and page 2, paragraph 0026).

Conclusion

15. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to ELENI A. SHIFERAW whose telephone number is (571)272-3867. The examiner can normally be reached on Mon-Fri 6:00am-2:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser R. Moazzami can be reached on (571) 272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Eleni A Shiferaw/
Primary Examiner, Art Unit 2436